PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Alan Dowd et al. Examiner: Dwin M. Craig

Serial No.: 09/483,127 Group Art Unit: 2123

Filed: January 14, 2000 Docket: 105.176US1

For: NETWORK SECURITY MODELING SYSTEM AND METHOD

APPEAL BRIEF UNDER 37 CFR § 41.37

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Appeal Brief is presented in support of the Notice of Appeal to the Board of Patent Appeals and Interferences, filed on August 18, 2005, from the Final Rejection of claims 1-42 of the above-identified application, as set forth in the Office Action mailed on April 18, 2005.

The Commissioner of Patents and Trademarks is hereby authorized to charge Deposit Account No. 19-0743 in the amount of 250.00 which represents the requisite fee set forth in 37 C.F.R. § 41.2(b)(2). The Appellants respectfully request consideration and reversal of the Examiner's rejections of pending claims 1-42.

02/28/2006 BABRAHA1 00000022 190743 09483127

02 FC:2254 795.00 DA

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest of the above-captioned patent application is the assignee, SECURE COMPUTING CORPORATION.

2. RELATED APPEALS AND INTERFERENCES

Appellants know of no other appeals or interferences which will have a bearing on the Board's decision in the present appeal.

3. STATUS OF THE CLAIMS

Claims 1-42 are pending; all of these claims have been rejected, and are the subject of the present appeal.

4. STATUS OF AMENDMENTS

All amendments have been entered. The last amendment was made in the Amendment and Response filed April 21, 2003.

5. SUMMARY OF CLAIMED SUBJECT MATTER

As noted in the Background of the present patent application, the amount of information being transferred between systems internal and external to a network continues to increase, creating a need for improved network security tools. Conventional network vulnerability tools do not look at the interactions between network components or show the path of an attack. These tools may not look at both the internal and external face of the network. Additionally, tools that assess vulnerabilities through controlled attacks on the network leave footprints such as log entries and may disrupt the network.

The present application describes a network securities modeling system, a method for assessing network vulnerabilities and a method for opposing network attackers. The system taught by Appellants and claimed in claims 1-17 and 34-42 uses a simulator in conjunction with a network configuration database and network vulnerabilities database to determine network security issues (p. 2, lines 21-22; Fig. 1).

The network configuration database contains a plurality of network tables such as a node table, routing table, configuration table, and filter table (p. 13, line 25 – p. 14, line 1). Network configuration data may be received from an objective network, the output of a network configuration discovery tool, or a system administrator (p. 11, lines 23 – 26). Stored network configuration data can be used to run multiple tests or attack strategies on a single network configuration. In one embodiment, a user is allowed to modify the network configuration data. This allows system administrators to either test the results of adding new components to an existing network or test the design of a non-existent network (p. 9, line 24 – p. 10, line 3). An illustration of one embodiment of the network configuration database is shown in Figure 7.

The network vulnerabilities database contains vulnerability data about conventional network components, hardware and software (p. 5, lines 10 – 12). Specifically, each entry contains the service including version and patch levels, defense conditions that might close the vulnerability, the resource and state conditions needed to exercise the vulnerability and the effects of exploiting the vulnerability (p. 17, lines 2-7).

Simulations are run to determine network vulnerabilities using vulnerability and network configuration data. The simulator is capable of simulating a variety of networks including enterprise networks, wide area networks and local area networks using the network configuration data (p. 5, lines 1-3). The simulator is also able to simulate network components such as servers, workstations, routers and firewalls, as well as the protocols and services that run on the components (p. 5, lines 3-5). The simulator analyzes interactions between network components, the interior and the exposed face of the network. Simulations can be preformed based on specific attack scenarios using configuration and vulnerability data, general attack scenarios, or attack scenarios determined by a system administrator or other user (p. 6, lines 15-17; p. 7, lines 6-9)

Appellants teach, and claim in claims 10-17, 34-37, 39 and 41-42, a mission objectives module coupled to the network simulator. The mission objectives module contains critical resource information such as goals, expectations, and constraints for simulating the network (p. 9, lines 1-3). The information may be used to determine that a particular entity is important for a specific attack scenario (p. 9, lines 3-5). Mission objectives data may be contained in a plurality of tables and modeled as components or services that need to be protected against attacks (p. 17, lines 25-32).

Appellants teach, and claim in claims 9, 38 and 39, the system implemented as an interactive computer game. The system may have a plurality of client players such as attackers, defenders, or administrators. (p. 20, lines 1-4). Clients attack the network by sending commands that simulate service functionality, change services or nodes, and exploit vulnerabilities (p. 20, lines 14-15). Clients defend network territory by adjusting the posture of nodes, setting router and firewall filtering policies, and resetting nodes or services that have been disabled or compromised (p. 20, lines 15-17). The system may be used either for entertainment or as a training tool to educate personnel involved with network security in building and protecting secure networks (p. 20, lines 5-7).

Appellants teach, and claim in claims 18-27, a method of analyzing computer network security using a modeling system. As shown at p. 2, lines 25-30, Figure 1and p. 4, line 28 through p. 7, line 26, the method comprises providing a network configuration of a computer network, simulating the network based on the configuration, and

determining vulnerabilities of the simulated network using the vulnerability information stored in the database.

Appellants teach, and claim in claims 28-33, a method of opposing network attackers. As shown at p. 3, lines 1-6, Figure 3 and p. 11, line 6-22, the method includes receiving a network configuration, receiving mission objectives, receiving commands from a network attacker, simulating the network based on the commands received from the attacker, and responding to the network attacker.

This summary does not provide an exhaustive or exclusive view of the present subject matter, and Appellants refer to the appended claims and its legal equivalents for a complete statement of the invention.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Are claims 1, 2, 4, 5, 8, 18 and 19 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat?

Are claims 3 and 6 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat and further in view of Gleichauf (U.S. Patent No. 6,282,546)?

Are claims 7 and 9 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat and in further view of Sparks II (U.S. Patent No. 6,352,479)?

Are claims 10, 11, 13, 14 and 16 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and in further view of Samfat, Bergman (U.S. Patent No. 6,442,694), and Smith Jr. (U.S. Patent No. 5,662,478)?

Are claims 12 and 15 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and in further view of Samfat, Bergman (U.S. Patent No. 6,442,694), and Smith Jr. (U.S. Patent No. 5,662,478) and further in view of Gleichauf (U.S. Patent No. 6,282,546)?

Is claim 17 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and in further view of Samfat, Bergman (U.S. Patent No. 6,442,694), and Smith Jr. (U.S. Patent No. 5,662,478) and further in view of Sparks II (U.S. Patent No. 6,352,479)?

Is claim 20 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent

No. 6,343,362), and in further view of Samfat and further in view of Ballard (U.S. Patent No. 4,937,825)?

Are claims 21-23 and 26 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat and Jackson?

Are claims 23, 24 and 25 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat, Jackson and Kurtzberg (U.S. Patent No. 5,961,644)?

Is claim 27 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and in further view of Samfat, Jackson and Gleichauf (U.S. Patent No. 6,282,546)?

Are claims 28-30 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Johnson, and in further view of Samfat, Kurtzberg (U.S. Patent No. 5,961,644), and Jackson?

Are claims 31-33 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Johnson, and in further view of Samfat, Kurtzberg (U.S. Patent No. 5,961,644), Jackson and Porras et al. (U.S. Patent No. 6,321,338)?

Are claims 34-38 and 40-42 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Johnson, in view of Porras (U.S. Patent No. 6,321,338), and in further view of Samfat and Gleichauf (U.S. Patent No. 6,282,546)?

Are claims 9 and 39 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat and Jackson?

Are claims 1-8, 10-15, 18-22, 25-37 and 40-42 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Kondo et al. (U.S. Patent No. 5,684,957) in view of Shostack et al. (U.S. Patent No. 6,298,445?

7. ARGUMENT

Rejections under U.S.C. § 103

1) The Applicable Law

According to *M.P.E.P.* § 2141, which cites *Hodosh v. Block Drug Co., Inc.*, 786 F.2d 1136, 1143 n.5, 229 USPQ 182, 187 n.5 (Fed. Cir. 1986), the following tenets of patent law must be adhered to when applying 35 U.S.C. § 103. First, the claimed invention must be considered as a whole. Second, the references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination. Third, the references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention. Fourth, obviousness is determined using a reasonable expectation of success standard. Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. *M.P.E.P.* § 2141 (citing *Graham v. John Deere*, 383 U.S. 1, 148 USPQ 459 (1966)).

The Examiner has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *M.P.E.P.* § 2142 (citing *In re Vaeck*, 947 F.2d, 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on Appellants' disclosure. *M.P.E.P.* § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). The references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the

references. *M.P.E.P.* § 2142 (citing *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)). In considering the disclosure of a reference, it is proper to take into account not only specific teachings of the reference but also the inferences which one skilled in the art would reasonably be expected to draw there from. *M.P.E.P.* § 2144.01 (citing *In re Preda*, 401 F.2d 825, 826, 159 USPQ 342, 344 (CCPA 1968)). However, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *M.P.E.P.* § 2143.01 (citing *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)).

In order to take into account the inferences which one skilled in the art would reasonably make, the examiner must ascertain what would have been obvious to one of ordinary skill in the art at the time the invention was made. *M.P.E.P.* § 2141.03 (citing *Environmental Designs, Ltd. v. Union Oil Co*, 713 F.2d 693, 218 USPQ 865 (Fed. Cir. 1983), *cert. denied*, 464 U.S. 1043 (1984)).

> The examiner must step backward in time and into the shoes worn by the hypothetical "person of ordinary skill in the art" when the invention was unknown and just before it was made. In view of all factual information, the examiner must then make a determination whether the claimed invention "as a whole" would have been obvious at that time to that person. Knowledge of Appellants' disclosure must be put aside in reaching this determination, yet kept in mind in order to determine the "differences," conduct the search and evaluate the "subject matter as a whole" of the invention. The tendency to resort to "hindsight" based upon Appellants' disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.

M.P.E.P. § 2141.03.

2) Application of §103 to the Rejected Claims

Claims 1, 2, 4, 5, 8, 18 and 19 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat. Appellant

respectfully submits that the Examiner has failed to meet his burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness.

As noted above, in order to establish a *prima facie* case of obviousness, the Examiner must meet three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

Gleichauf describes a system and method for characterizing a network and identifying vulnerabilities. As noted by the Examiner, Gleichauf discloses a network configuration module having network configuration data. In contrast to Appellants, however, Gleichauf identifies and tests vulnerabilities by applying a rule set (col. 4, lines 43-47, col. 7, lines 6-31 and Fig. 4) to identify vulnerabilities and then testing the actual network to see if the vulnerabilities exist.

Appellants teach that it can be difficult to test vulnerabilities on the network itself. As noted on p. 1, lines 28-30, such tests can disrupt the network and may leave footprints such as event log entries and the like on scanned machines. Therefore, in contrast to Gleichauf, Appellants teach, and claim in claims 1-42, the use of a separate security modeling system which uses a simulator to identify and test vulnerabilities.

The Examiner acknowledges that Gleichauf does not disclose a network simulation for analyzing attacks against a network but states that Ptacek "discloses a network simulation for analyzing attacks against a network." Appellants disagree.

Ptacek describes a higher-level computer language that can be used to create programs that simulate attacks against a computer network. The Examiner is confusing the simulation described by Ptacek with the simulation performed by Appellant. In contrast to Appellant, Ptacek describes how a higher-level language can be used to generate network traffic in order to test an existing network with known attacks. Ptacek does not, therefore, describe a network simulation for analyzing attacks against a network, but instead describes a computer language for generating such attacks against the network itself.

Appellant therefore agrees with the Examiner that the combination of Gleichauf and Ptacek still fails to teach a key limitation of claims 1-42, the simulator itself.

The Examiner stated that Gleichauf does not disclose a network simulation. The Examiner stated that Samfat "discloses a network simulation."

Samfat describes a mobile network simulator used to test software applications in a mobile telephone environment. Samfat notes that it can be difficult to test software in the early stages of network development and that, even if a network is available, it would be difficult and expensive to generate the traffic needed to test such a network. Samfat notes that these problems can be overcome by the use of simulators. Samfat describes a Global System for Mobile (GSM) telephone network simulation model and uses that model to test a dedicated Network Management System whose main purpose is to provide intrusion detection services. Samfat, p. 766.

The Examiner stated that it would have been obvious to combine Gleichauf with Samfat because, "by being able to exactly repeat the manner in which the network behaves as the attack takes place, software counter measures can be tested, and then retested in an environment where the same conditions can be repeated when debugging the counter measure software," (Office Action, p. 9, citing to Samfat p. 766 "These problems [the problems of testing software deployed across widespread networks] can be overcome by the use of simulators which also present the advantage of exact repeatability of successive runs (useful during software implementation)."). There is no support in any of the cited references for this position. Furthermore, the Examiner has failed to establish at even a prima facie level that one of ordinary skill in the art at the time of the invention would be moved to combine Gleichauf, Ptacek and Samfat in the manner suggested by the Examiner. Instead, the Examiner has fallen into the trap of depending on Appellant's disclosure and a fair amount of hindsight to craft his rejection.

Even if the references are combined in the manner suggested by the Examiner, the combination does not teach the claimed invention. As noted above, the prior art references, when combined, must teach or suggest all the claim limitations. Even if Gleichauf teaches a method of identifying potential vulnerabilities, Gleichauf does not disclose simulating and/or analyzing the network vulnerabilities database as required by

claims 1-42, instead limiting the active analysis phase to verifying the existence of vulnerabilities determined by acting upon the configuration database with a rule set (Col. 8, lines 13-18).

In comparison, Appellants teach that the simulator can be used to "simulate and analyze networks based on the network configuration data" as claimed in claims 1-17 or to simulate "the network based on the network configuration" and to determine "vulnerabilities of the simulated network" as described by Appellant and claimed in claims 18-27.

The Examiner stated that Gleichauf discloses

> a computer implemented method of analyzing networks based on the network configuration data where the software includes a network vulnerabilities database where the network vulnerabilities database includes, a plurality of known network vulnerabilities where each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

Office Action p. 8. Appellant respectfully disagrees.

The system described by Gleichauf creates a network vulnerabilities database using rules applied to information in the port database. Gleichauf teaches using three rules; the first to determine an operating system, the second to determine a service and the third to determine a potential vulnerability. Thus, while Gleichauf describes a database of network vulnerabilities organized in a hierarchical structure where each entry contains an operating system represented by the entry, a service to which it applies and a potential vulnerability, the reference does not teach that these vulnerabilities include "defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability" as required by claims 1-27.

The bottom line is that Gleichauf describes a network that can analyze its own vulnerabilities, Ptacek describes a system and method for generating raw network packets that can be used to test a network and Samfat describes using a simulator to debug software. There is no teaching or motivation to combine the traffic generation software of Ptacek with the network analysis of Gleichauf and the network simulation of Samfat to form the security modeling system of Appellant.

Appellants respectfully request that the Examiner's rejection of claims 1-8 and 18-27 be reversed.

Claims 3 and 6 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat and further in view of Gleichauf (U.S. Patent No. 6,282,546, hereinafter "G2").

Gleichauf, Ptacek, and Samfat are discussed above. As noted above none of the references teach a security modeling system having a simulator as claimed by Appellants. Also, the combination of the references is non-obvious, as previously discussed. Claims 3 and 6 are patentable for the reasons given for claims 1-8 and 18-27 above.

Claims 7 and 9 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat and in further view of Sparks II (U.S. Patent No. 6,352,479, hereinafter "Sparks II")?

Gleichauf, Ptacek, and Samfat are discussed above. As noted above none of the references teach a security modeling system having a simulator as claimed by Appellants. Also, the combination of the references is non-obvious, as previously discussed. Claims 7 and 9 are patentable for the reasons given for claims 1-8 and 18-27 above.

Sparks II describes a system for screening players in an online multiplayer game system. Sparks teaches that by screening players, the players are more likely to compete against opponents of equal skill level with preferences agreeable to most of the players involved. Even if Sparks II describes an attacker and a defender in the context of an Internet-based game, there is no teaching or motivation in any of the cited references to create an environment where an attacker can attack a computer network through a simulation of that network and a defender can defend that same simulated network.

The Examiner stated that it would be obvious to one of ordinary skill in the art to add a defender and attacker user interface to the security modeling system of claim 1 as described by Appellant and claimed in claim 7 because "by supporting multiple players using a network and graphical user interfaces, complex and real-time interaction between an attacker and a defender can be achieved over great distances using a network, like the

internet...". There is no support in any of the cited references for this position. Furthermore, the Examiner has failed to establish at even a prima facie level that one of ordinary skill in the art at the time of the invention would be moved to combine Gleichauf, Ptacek, Samfat and Sparks II in the manner suggested by the Examiner. Instead, the Examiner has fallen into the trap of depending on Appellant's disclosure and a fair amount of hindsight to craft his rejection.

Appellants respectfully request that the Examiner's rejection of claim 7 be reversed.

The Examiner stated that it would be obvious to one of ordinary skill in the art to create a game such as claimed in claim 9 because "by playing a game using the game server disclosed in Sparks II reference the player is able to be handicapped in a manner to determine the current level of skill and this is useful in determining if that particular individual is ready for operating at a particular skill level. In the manner described a computer security expert could determine if a particular person is qualified to receive a certification for a particular job protecting a computer network." There is no support in any of the cited references for this position. Furthermore, the Examiner has failed to establish at even a prima facie level that one of ordinary skill in the art at the time of the invention would be moved to combine Gleichauf, Ptacek, Samfat and Sparks in the manner suggested by the Examiner. Instead, the Examiner has fallen into the trap of depending on Appellant's disclosure and a fair amount of hindsight to craft his rejection. Note that the language the Examiner is using for his motivation to combine Sparks II with the other references appears to be lifted from Appellant's own specification. "In one embodiment, the security modeling system is a training tool used to educate system administrators, information technology managers and other users on how to build and protect secure networks." Specification, p.20, lines 5-7.

Appellants respectfully request that the Examiner's rejection of claim 9 be reversed.

Claims 10, 11, 13, 14 and 16 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of

Ptacek (U.S. Patent No. 6,343,362), and in further view of Samfat, Bergman (U.S. Patent No. 6,442,694), and Smith Jr. (U.S. Patent No. 5,662,478)?

Gleichauf, Ptacek, and Samfat are discussed above. As noted above none of the references teach a security modeling system having a simulator as claimed by Appellants. Also, the combination of the references is non-obvious, as previously discussed. Claims 10, 11, 13, 14 and 16 are patentable for the reasons given for claims 1-8 above.

The Examiner stated that Gleichauf does not disclose a mission objectives module coupled to the simulator used to determine network components that are involved in a specific attack scenario. The Examiner stated that Bergmann discloses determining network components that are involved in a specific attack scenario.

Bergmann describes a method and a system for isolating faults in high speed communications networks. Bergmann teaches that the inability to determine if a fault is caused by an attack or failure coupled with the inability to determine the source of an attack can result in unnecessary shutdowns and delays. While Bergmann has relevance in network security applications, the system does not serve the purpose that the Appellants' mission objective module does in determining components involved in an attack scenario. Appellants teach knowing which components are likely to be involved in an attack scenario before and after the simulation is run in order to assess the security of the network. In contrast, Bergmann teaches a defensive method and system for protecting the integrity and efficiency of a network against an attack in progress.

Appellants described, and claims in claims 10-17, using "critical resource information ... to determine network components that are involved in a specific attack scenario." Berman, on the other hand, ascertains whether an attack is caused by network traffic, or from a failure in a component on the network. There is no analysis in Bergman of critical resource information used "to determine network components that are involved in a specific attack scenario" as described by Appellant and claimed in claims 10-17.

The Examiner stated that Smith Jr. discloses mission objectives. Smith Jr. describes a tool useful in creative thinking sessions. Regardless of whether Smith Jr. teaches mission objectives, or missions and objectives, they are of a distinctly different character than the mission objectives module Appellants disclose. Missions and

objectives in the context of Smith Jr. relate to generic problem solving goals. In contrast, Appellants teach mission objectives of a different kind, used to determine which components are involved in a specific network simulation and including critical resource information.

No combination of the references teaches a mission objectives module coupled to the simulator used to determine the network components that are involved in specific attack scenarios. Appellants respectfully request that the Examiner's rejection of claims 10-17 be reversed.

Claims 12 and 15 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and in further view of Samfat, Bergman (U.S. Patent No. 6,442,694), and Smith Jr. (U.S. Patent No. 5,662,478) and further in view of Gleichauf (U.S. Patent No. 6,282,546).

Gleichauf, Ptacek, Samfat, Berman, Smith and G2 are discussed above. As noted above none of the references teach a security modeling system having a simulator as claimed by Appellants. Also, the combination of the references is non-obvious, as previously discussed. Claims 12 and 15 are patentable for the reasons given for claims 10, 11, 13, 14 and 16 above.

Claim 17 was rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and in further view of Samfat, Bergman (U.S. Patent No. 6,442,694), and Smith Jr. (U.S. Patent No. 5,662,478) and further in view of Sparks II (U.S. Patent No. 6,352,479).

Gleichauf, Ptacek, Samfat, Berman, Smith and Sparks II are discussed above. As noted above none of the references teach a security modeling system having a simulator as claimed by Appellants. Also, the combination of the references is non-obvious, as previously discussed. Claim 17 is patentable for the reasons given for claims 10, 11, 13, 14 and 16 above.

In addition, the Examiner stated that it would be obvious to one of ordinary skill in the art to add a defender and attacker user interface to the security modeling system of

claim 10 as described by Appellant and claimed in claim 17 because "by supporting multiple players using a network and graphical user interfaces, complex and real-time interaction between an attacker and a defender can be achieved over great distances using a network, like the internet...". There is no support in any of the cited references for this position. Furthermore, the Examiner has failed to establish at even a prima facie level that one of ordinary skill in the art at the time of the invention would be moved to combine Gleichauf, Ptacek, Samfat, Berman, Smith and Sparks II in the manner suggested by the Examiner. Instead, the Examiner has fallen into the trap of depending on Appellant's disclosure and a fair amount of hindsight to craft his rejection.

Appellants respectfully request that the Examiner's rejection of claim 17 be reversed.

Claim 20 was rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and in further view of Samfat and further in view of Ballard (U.S. Patent No. 4,937,825).

Gleichauf, Ptacek, and Samfat are discussed above. As noted above none of the references teach a security modeling system having a simulator as claimed by Appellants. Also, the combination of the references is non-obvious, as previously discussed. Claim 20 is patentable for the reasons given for claims 18-27 above. Appellants respectfully request that the Examiner's rejection of claim 20 be reversed.

Claims 21-23 and 26 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat and Jackson?

Gleichauf, Ptacek, and Samfat are discussed above. As noted above none of the references teach a security modeling system having a simulator as claimed by Appellants. In addition, none of the references, alone or in combination, teach using mission objectives and the network configuration to simulate a network. Finally, the combination of the references is non-obvious, as previously discussed. Claims 21-23 and 26 are patentable for the reasons given for claims 18-27 above.

The Examiner stated that, although Gleichauf does not disclose mission objective, the Jackson reference discloses mission objectives. For support the Examiner turns to the section entitled "Winning the Game" on p. 7 of the Jackson reference. Even if what Jackson discloses could be construed as a "mission objective" the Examiner failed to show how the network could be simulated "based on the network configuration and mission objectives" as required by claim 21. Since a limitation of claim 21 is not present in any of the references, the Examiner has failed to establish a *prima facie* case of obviousness. Appellants respectfully request that the Examiner's rejection of claim 21 be reversed.

The Examiner seems to have erred in his rejection of claim 22 under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat and Jackson. It appears that he may have intended to reject claim 22 under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat, since he doesn't use the Jackson reference in his rejection and he used Samfat previously to provide the missing simulator. It really doesn't matter, however, since, as noted above, none of the references teach a security modeling system having a simulator, nor the use of a graphical user interface to interact with that simulator, as claimed by Appellants in claim 22. In addition, the combination of the references is non-obvious, as previously discussed, and claim 22 is patentable for the reasons given for claims 18-27 above.

In his rejection of claim 23, the Examiner stated that, although Gleichauf does not disclose dynamically interacting with an attacker, Jackson discloses interacting with an attacker. Jackson does not, however, as noted above, either teach the use of a graphical user interface to modify the simulation or the use of the user interface to dynamically interact with an attacker as required by claim 23. Since key limitations of claim 23 are not present in any of the references, the Examiner has failed to establish a *prima facie* case of obviousness. Appellants respectfully request that the Examiner's rejection of claim 23 be reversed.

In his rejection of claim 26, the Examiner stated that, although Gleichauf does not disclose a score, Jackson discloses a score. Once again the Examiner ignores key limitations of the claims. The limitation in claim 26 is "wherein determining vulnerabilities includes computing security results, wherein the security results include a security score." The term "security score" is defined in the specification at p.7, lines 10-15,

> The security modeling system 100 scores the security system based on its effectiveness in defending critical resources. In an alternate embodiment, the security modeling system 100 scores the security system by measuring the effectiveness based on its ability to defend critical resources with the least amount of time and resources expended.

The "score" of Jackson is the score in a card game. Since key limitations of claim 26 are not present in any of the references, the Examiner has failed to establish a *prima facie* case of obviousness. Appellants respectfully request that the Examiner's rejection of claim 26 be reversed.

Claims 23, 24 and 25 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat, Jackson and Kurtzberg (U.S. Patent No. 5,961,644)?

Kurtzberg, like Ptacek, describes a simulated attack on a computer network. Like Ptacek, Kurtzberg uses known attacks to test an existing network.

As in his rejection of claim 23 above, the Examiner stated that, although Gleichauf does not disclose dynamically interacting with an attacker, Kurtzberg discloses interacting with an attacker. Kurtzberg, does not however, do as the Examiner states. Instead, Kurtzberg simulates an attack on a real system. The only output is in the form of alarms to key security personnel.

In addition, Kurtzberg does not either teach the use of a graphical user interface to modify the simulation or the use of the user interface to dynamically interact with an attacker as required by claim 23. Since key limitations of claim 23 are not present in any

of the references, the Examiner has failed to establish a *prima facie* case of obviousness. Appellants respectfully request that the Examiner's rejection of claim 23 be reversed.

In his rejection of claims 24 and 25, the Examiner states that, although Gleichauf does not disclose interacting in real time with a security modeling system, Kurtzberg does disclose interacting in real time with a security modeling system. Appellant disagrees. As noted above, Kurtzberg executes software that tests an existing network, not a simulation of the network. Kurtzberg cannot, therefore, interact in real time with a security modeling system as that term is described and claimed by Appellant in claims 24 and 25. In addition, claims 24 and 25 are patentable for the reasons given for claims 22 and 23 above. Appellants respectfully request that the Examiner's rejection of claims 24 and 25 be reversed.

Claim 27 was rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and in further view of Samfat, Jackson and Gleichauf (U.S. Patent No. 6,282,546).

Claim 27 is patentable for the reasons given for claim 21 above. Appellants respectfully request that the Examiner's rejection of claim 21 be reversed.

Claims 28-30 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Johnson, and in further view of Samfat, Kurtzberg (U.S. Patent No. 5,961,644), and Jackson.

Gleichauf and Samfat are discussed above. As noted above none of the references teach a simulator similar to that claimed by Appellants. Also, the combination of the references is non-obvious.

The Examiner stated that Jackson discloses mission objectives. Jackson describes mission objectives in the context of gaining access to a given number of systems in order for a player to win a game. In contrast, Appellants teach using mission objectives that include critical resource information in order to determine components involved in a specific attack scenario. In addition, there is no motivation to combine the references, because Jackson does not teach an accurate model of a network, but rather a stylized card game using hacker terminology.

No combination of the references teaches receiving mission objectives including critical resource information used to determine network components that are involved in a specific attack scenario as required by claims 28-34. None of the references teach simulating a network as a function of network configuration, mission objectives and stored vulnerability data as required by claims 28-34. No combination of references teaches responding to the network attacker by imposing barriers, providing response messages and protecting the network as described by Appellant and claimed in claims 28-34. Furthermore, no combination of the references teaches receiving commands from a defender and simulating execution of the commands to determine results based on the defender commands are described by Appellant and claimed in claim 29. Appellants respectfully request that the Examiner's rejection of claims 28-30 be reversed.

Claims 31-33 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Johnson, and in further view of Samfat, Kurtzberg (U.S. Patent No. 5,961,644), Jackson and Porras et al. (U.S. Patent No. 6,321,338).

Claims 31-33 are patentable for the reasons given for claims 28-34 above.

In addition, none of the references teach modifying the simulation using a graphical user interface, as required by claims 31-33, or computing a security score as required by claim 32. The term "security score" is defined in the specification at p.7, lines 10-15,

> The security modeling system 100 scores the security system based on its effectiveness in defending critical resources. In an alternate embodiment, the security modeling system 100 scores the security system by measuring the effectiveness based on its ability to defend critical resources with the least amount of time and resources expended.

Appellants respectfully request that the Examiner's rejection of claims 31-33 be reversed.

Claims 34-38 and 40-42 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Johnson, in view of Porras (U.S. Patent No. 6,321,338), and in further view of Samfat and G2.

Samfat is discussed above. As noted above, the reference does not teach a simulator similar to that claimed by Appellants.

The Examiner stated that Johnson "discloses a security modeling system for simulating networks and to determine network components that are involved in a specific attack scenario including configuration data," (Office Action, p. 28). Appellants disagree. Johnson, like Ptacek and Kurtzberg, discloses a system that launches attacks against an existing network in order to determine possible vulnerabilities. Johnson also teaches obtaining information such as which network components are involved in a specific attack and configuration data through a controlled attack on an existing network. However, Johnson does not teach a security modeling system for simulating networks.

The Examiner stated that Samfat describes a network simulator and that it would be obvious to combine Johnson and Samfat to form the network simulator described and claimed by Appellant. Appellant respectfully submits that there is no teaching in either of the references that would lead one to combine the references to form the simulator described and claimed by Appellant.

The Examiner stated that Gleichauf 2 discloses a plurality of data bases including mission objective tables, vulnerability tables and network configuration tables. Gleichauf 2 describes a system and method for inserting data into a multi-dimensional database in real time. Gleichauf 2 discusses the application of this system to network intrusion detection and vulnerability assessment systems. While Gleichauf 2 does disclose vulnerability tables and network configuration tables, the reference does not disclose mission objective tables. Appellants teach that mission objective tables are a valuable tool in determining attack scenarios and also for evaluating network security.

In his rejection of claim 38, the Examiner stated that although Johnson does not transmit real-time network information, Porras discloses real-time monitoring. Claim 38 is dependent on claim 9. The Examiner has failed to show how either Johnson or Porras teach a computer game having a network configuration module or a simulator coupled to the network configuration module as required by claim 9. In addition, the real-time monitoring described by Porras is limited to real-time analysis of network packets. The Examiner has failed to provide a reference describing a simulator with "an

attacker interface to transmit real-time network status information to an attacker during a simulation" and "a defender interface to transmit real-time network status information to a defender during a simulation" as described by Appellant and as required by claim 38.

Appellants respectfully request that the Examiner's rejection of claims 34-38 and 40-42 be reversed.

Claims 9 and 39 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and further in view of Samfat and Jackson.

Gleichauf, Ptacek, and Samfat are discussed above. As noted above none of the references teach a simulator similar to that claimed by Appellants. Also, the combination of the references is non-obvious, as previously discussed.

The Examiner stated that Gleichauf did not disclose a computer game. The Examiner stated that Jackson discloses a game, and Sparks discloses a computer game.

Jackson describes a card game based on the Illuminati system. The card game uses hacker terminology to create a game in which players try to gain access to one or more cards representing computer systems. The game described by Jackson builds a network during game play by laying cards down in a domino-like manner. However, the use of hacker and network terminology in the game is a superficial change of a pre-existing card game (compare Jackson to Jackson2).

In contrast, Appellants teach a game with a modeled network that behaves accurately enough to train system administrators and other personnel on how to build and protect secure networks (p. 20, lines 5-7). Such a game requires the use of a network configuration module and a simulator coupled to the network configuration module to simulate the network, as required by claims 9, 38 and 39.

The Examiner stated that combining Gleichauf with Jackson would have been obvious because Jackson shows "modeling a computer network and pretending to hack into that network are activities that people like to do." While Jackson does teach that playing an Illuminati style card game is something people like to do, the reference does not show that playing a computer game involving attacking or defending an accurate simulation of a realistic network was described prior to the invention by Appellants.

Appellants respectfully submit that the Examiner relied on the Appellants' disclosure and/or impermissible hindsight in forming the rejection of claims 9, 38 and 39 over the cited references. As such, Appellants respectfully request that the Examiner's rejection of claims 9, 38 and 39 be reversed.

Claims 1-8, 10-15, 18-22, 25-37 and 40-42 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Kondo et al. (U.S. Patent No. 5,684,957) in view of Shostack et al. (U.S. Patent No. 6,298,445.

Kondo describes a variety of mechanism for monitoring status of a network of computers. Kondo describes a mechanism by which devices in a network can monitor network traffic and transmit the information gathered to a network management system. Kondo, col. 15, line 53- col. 16, line 26. Kondo also describes a mechanism by which login procedures can be tracked on individual computers (col. 17, line 28 – col. 18, line 19), a mechanism by which the history of file accesses can be tracked (col. 18, line 20 – col. 19, line 8), and a mechanism by which a log can be made of program activations (col. 19, lines 9-20). All of these mechanisms execute on the actual network being monitored. Any of these logs can be monitored for improper activity.

The Examiner stated that Kondo discloses a network simulation and model for use in intrusion detection of a computer network. None of the sections cited by the Examiner, however, discuss simulation of a network. Appellant was unable, after careful reading of Kondo, to find any mention of network simulation. Kondo instead operates on the network being monitored as noted above.

As noted by the Examiner, Kondo also lacks a database of network vulnerabilities as described by Appellant and claimed in claims 1-42. Instead, Kondo monitors and then analyzes the results of the monitoring. The Examiner stated that Shostack discloses a database of network vulnerabilities in Fig. 6, element 92.

As noted above, in order to establish a *prima facie* case of obviousness, the Examiner must meet three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings.

Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

The combination of Kondo and Shostack fails to show a security modeling system having "a network configuration module having network configuration data" and "a simulator coupled to the network configuration module to simulate and analyze networks based on the network configuration data" as required by claims 1-17. Furthermore, the combination of references fails to show a simulator that "includes a network vulnerabilities database, and wherein the network vulnerabilities database includes a plurality of known network vulnerabilities, wherein each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability" as required by claims 1-8, 10-17, 18-27 and 40-42.

The combination of Kondo and Shostack fails to show a method of opposing network attackers. Neither reference shows "simulating the network based on the commands received from the network attacker" as required by claims 28-33 and neither reference shows a simulator having a plurality of databases as required by claims 34-37.

Appellants respectfully request that the Examiner's rejection of claims 1-8, 10-15, 18-22, 25-37 and 40-42 be reversed.

It is respectfully submitted that the cited art neither anticipates or renders the claimed invention obvious and that therefore the claimed invention does patentably distinguish over the cited art. It is respectfully submitted that claims 1-42 should therefore be allowed. Reversal of the Examiner's rejections of claims 1-42 is respectfully requested.

Respectfully submitted,

ALAN DOWD et al.

By their Representatives,

SCHWEGMAN, LUNDBERG,
WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402

Date Feb 22, 2006 By Thomas J. Brennan
Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Appeal Brief, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 22nd day of February, 2006.

Amy Moriarty
Name

Signature

CLAIMS APPENDIX

1. (Rejected) A security modeling system comprising:

a network configuration module having network configuration data;

a simulator coupled to the network configuration module to simulate and analyze networks based on the network configuration data, wherein the simulator includes a network vulnerabilities database, and wherein the network vulnerabilities database includes:

a plurality of known network vulnerabilities, wherein each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

2. (Rejected) The system of claim 1, wherein the network vulnerabilities database includes network vulnerability, attack and exploitation data.

3. (Rejected) The system of claim 2, wherein the network configuration data and the network vulnerability, attack and exploitation data are stored in database tables and the data is processable by a computer.

4. (Rejected) The system of claim 1, wherein the network configuration module comprises network configuration data output by a network configuration discovery tool.

5. (Rejected) The system of claim 1, wherein the simulator includes a graphical user interface.

6. (Rejected) The system of claim 2, wherein the simulator includes a means for receiving the network vulnerability, attack and exploitation data.

7. (Rejected) The system of claim 1, wherein the simulator includes a defender and an attacker user interface.

8. (Rejected) The system of claim 1, wherein the security modeling system is portable.

9. (Rejected) A computer game comprising:

a network configuration module having network configuration data;

a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database, and wherein the simulator includes a graphical user interface for playing the game.

10. (Rejected) A security modeling system comprising:

a network configuration module having network configuration data;

a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database; and

a mission objectives module coupled to the simulator, wherein the mission objectives module includes critical resource information used to determine network components that are involved in a specific attack scenario.

11. (Rejected) The system of claim 10, wherein the network vulnerabilities database includes network vulnerability, attack and exploitation data.

12. (Rejected) The system of claim 11, wherein the network configuration data and the network vulnerability, attack and exploitation data is stored in database tables and the data is processable by a computer.

13. (Rejected) The system of claim 10, wherein the simulator includes a graphical user interface.

14. (Rejected) The system of claim 10, wherein the critical resource information includes goals, expectations and constraints for simulating the network.

15. (Rejected) The system of claim 10, wherein the simulator includes a means for receiving the network vulnerability, attack and exploitation data.

16. (Rejected) The system of claim 10, wherein the security modeling system is portable.

17. (Rejected) The system of claim 10, wherein the simulator includes a defender and an attacker interface.

18. (Rejected) A method of analyzing a computer network using a security modeling system, wherein the security modeling system includes a database of network vulnerability information, the method comprising:

providing a network configuration of a computer network;

simulating the network based on the network configuration; and

determining vulnerabilities of the simulated network using the vulnerability information stored in the database, wherein the database includes a plurality of known network vulnerabilities, wherein each network vulnerability includes:

a plurality of known network vulnerabilities, wherein each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

19. (Rejected) The method of claim 18, wherein providing a network configuration includes receiving a configuration as the output of a network discovery tool.

20. (Rejected) The method of claim 18, wherein providing a network configuration includes receiving a data file which includes a configuration of the computer network.

21. (Rejected) The method of claim 18, wherein simulating the network includes:

receiving mission objectives;

storing the objectives; and

simulating the network based on the network configuration and mission objectives.

22. (Rejected) The method of claim 21, wherein determining vulnerabilities includes modifying the simulation using a graphical user interface.

23. (Rejected) The method of claim 22, wherein modifying the simulation includes dynamically interacting with an attacker.

24. (Rejected) The method of claim 22, wherein modifying the simulation includes dynamically interacting in real time with the security modeling system.

25. (Rejected) The method of claim 23, wherein modifying the simulation includes dynamically interacting in real time with the security modeling system.

26. (Rejected) The method of claim 21, wherein determining vulnerabilities includes computing security results, wherein the security results include a security score.

27. (Rejected) The method of claim 21, wherein determining vulnerabilities of the simulated network includes updating the vulnerabilities database when vulnerabilities are detected.

28. (Rejected) A method of opposing network attackers comprising:

receiving a network configuration, wherein the network configuration comprises computer hardware and software component information;

receiving mission objectives including critical resource information used to determine network components that are involved in a specific attack scenario;

receiving commands from a network attacker;

simulating the network based on the commands received from the network attacker, wherein simulating the network includes determining results as a function of the network configuration, mission objectives and stored vulnerability data for the described computer hardware and software components; and

responding to the network attacker, wherein responding to the attacker includes imposing barriers, providing response messages and protecting the network.

29. (Rejected) The method of claim 28, wherein simulating the network further includes receiving commands from a defender and determining results based on the defender commands.

30. (Rejected) The method of claim 28, wherein receiving configuration includes receiving critical resource information, wherein the critical resource information includes goals, expectation and constraints for simulating the network.

31. (Rejected) The method of claim 28, and further includes modifying the simulation using a graphical user interface.

32. (Rejected) The method of claim 31, wherein determining vulnerabilities includes computing security results which include a security score.

33. (Rejected) The method of claim 31, wherein receiving commands includes receiving attack actions which include commands that simulate service functionality, commands that change services or nodes, and commands that exploit vulnerabilities.

34. (Rejected) A security modeling system for simulating objective networks comprising:

a simulator having a plurality of databases, wherein the plurality of databases include mission objectives tables including information used to determine network components that are involved in a specific attack scenario, vulnerability tables, and network configuration tables, wherein the network configuration tables include network configuration data; and

a graphical user interface which operates with the simulator to allow input and output to clients.

35. (Rejected) The system of claim 34, wherein the mission objectives tables include mission tables, mission files tables and mission services tables.

36. (Rejected) The system of claim 34, wherein the vulnerability tables include service tables.

37. (Rejected) The system of claim 34, wherein the network configuration tables include configuration tables, defense tables, filter tables, node tables, routing tables and password tables.

38. (Rejected) The computer game of claim 9, wherein the simulator further comprises:

an attacker interface to transmit real-time network status information to an attacker during a simulation; and

a defender interface to transmit real-time network status information to a defender during a simulation.

39. (Rejected) The computer game of claim 9 further comprising:

a mission objectives module coupled to the simulator, wherein the mission objectives module includes critical resource information used to determine network components that are involved in a specific attack scenario.

40. (Rejected) A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

providing a network configuration of a computer network;

simulating the network based on the network configuration; and

determining vulnerabilities of the simulated network using the vulnerability information stored in the database, wherein the database includes:

a plurality of known network vulnerabilities, wherein each network vulnerability includes the service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

41. (Rejected) The machine-readable medium of claim 40, wherein simulating the network includes:

receiving mission objectives;

storing the objectives; and

simulating the network based on the network configuration and mission objectives.

42. (Rejected) The machine-readable medium of claim 41, wherein mission objectives include critical resource information used to determine network components that are involved in a specific attack scenario.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.